UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,846	06/23/2003	Partha Bhattacharya	11353-0004-999	9310

24341 7590 01/24/2005

MORGAN, LEWIS & BOCKIUS, LLP.
2 PALO ALTO SQUARE
3000 EL CAMINO REAL
PALO ALTO, CA 94306

EXAMINER	
FLEARY, CAROLYN FATIMAH	

ART UNIT	PAPER NUMBER
2152	

DATE MAILED: 01/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

BEST AVAILABLE COPY

Office Action Summary	Application No.	Applicant(s)	
	10/602,846	BHATTACHARYA ET AL.	
	Examiner	Art Unit	
	Carolyn F. Fleary	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

a. **Claims 6, 7, 17,19, 25, and 31 are** rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

i. **Claim 6** recites the limitation "the pre-mapping and/or post-mapping domains" in line 1. There is insufficient antecedent basis for this limitation in the claim.

b. **Claim 7** recites the limitations

- "whose pre-mapping parameters" in line 3,
- "the post-
  mapping parameter domain " in line 5-6,
- "whose post-mapping parameter domain" in line 8,
- "the pre-mapping parameter domain" in line 10".

There is insufficient antecedent basis for these limitations in the claim.

c. **Claim 17** recites the limitation "the pre-mapping and/or post-mapping domains" in line 1. There is insufficient antecedent basis for this limitation in the claim.

d. **Claim 19** recites the limitations:

- "whose pre-mapping parameters" in line 3,
- "the post-mapping parameter domain " in line 5-6,
- "whose post-mapping parameter domain" in line 8,

- "the pre-mapping parameter domain" in line 10-11".

There is insufficient antecedent basis for these limitations in the claim.

e. **Claim 25** recites the limitation "the event's network session relationship" lines 11-12". There is insufficient antecedent basis for this limitation in the claim.

There is insufficient antecedent basis for these limitations in the claim.

f. **Claim 31** recites the limitations:

- "whose pre-mapping parameters" in line 3,
- "the post-mapping parameter domain " in line 5-6,
- "whose post-mapping parameter domain" in line 8,
- "the pre-mapping parameter domain" in line 10-11".

There is insufficient antecedent basis for this limitation in the claim.

All claims not explicitly mentioned above are rejected to by virtue of their dependency.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 1-5,8-13, 15-17, 20-29 and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paunikar et al. (US 2004/0073704) in view of Fink et al (US 6,496,935).

a. **In regards to claim 1,** Paunikar et al. discloses a method of grouping network events, comprising:

i. receiving a stream of network events ([0040] lines 1-3), each network event including a set of event parameters (i.e. network address, protocol) in association with a network session that corresponds (i.e. correlates) to a message being transmitted through a network ([0042] Lines 5-18);

ii. for a network event in the stream, making an initial session (i.e. connection) determination by determining whether the event (i.e data packets) belongs to a same network session as any previously received event ([0045] lines 1-8);

iii. for the network event, identifying information of network address translations performed by one or more devices along a network transmission path associated with the network event [0045] lines 12-17);

iv. categorizing the network event in accordance with at least one of the session determination and the network address translation (NAT) information ([0026],[0046]lines 5-13, figure 4); and

v. at a predefined time [0032],

(1) processing a categorized network event to identify another categorized network event, if any, belonging to a same network session as the categorized network event ([0026][0045]);

(2) grouping the categorized (i.e. based on protocol and network address) network event and the identified other categorized network event, if any, into a set [0046];

(3) and assigning a unique identifier (i.e. IP address and protocol provided) to the set of events that includes the categorized network event [0046].

Paunikar et al., teaches a log that contains data on all current sessions, which includes session data such as times [0032]. However Paunikar fails to explicitly teach predefined time to perform (1)-(3) above.

In related art, Fink et al. teaches a system that filters steam of events (i.e packets) and determines the destination to which the event will be forwarded to (col 2 lines 27-39). The system includes a source from which the stream of events initiates, a destination for receiving events and a NAT component (figure 1-#18, col 6 lines 65-67, col 7 lines 1-11) for filtering the events based on rules (col 2 lines 61-63). A NAT component (fig 1-#30).performs event (i.e packet) comparison to determine if the events belong to the same session (col 4 lines 26-33). The NAT component continues to monitor event activity as well as continues to perform the comparisons and if an event is not received within predefined period of time a timeout occurs and the connection is closed (col 4 lines 51-64).

It would have been obvious to one of ordinary skill in the art at the time of invention to perform (1)- (3) above of the Paunikar et al. system within a predefined time in order to, based on event activity, to prevent unexpected disconnection by determining whether to keep or

close a session (col 10, lines 18-27) thereby only allowing permitted events on a private (i.e. protected) network (col 5 lines 41-59).

b. **In regards to claim 2,** Paunikar et al. discloses the method of claim 1 as modified above, wherein the set of event parameters include:

- source address, destination address, and network protocol [0033].

Paunikar et al. is silent on source port and destination port.

Fink et al. teaches a connection (i.e. session) as a plurality of parameters, which describe the data transmission to which a packet (i.e events) belongs. Parameters include source address and port of packet; destination address and port of the packet; protocol of the packet and interface from which the packet was received. The connection is used to classify the packet, and to determine whether the packet is permitted to enter and leave the protected network (col 6 lines 54-63).

It would be obvious to one of ordinary skill in the art at time of the invention to indicate the event parameters of Paunikar et al. as including such parameters in order to perform an initial session determination and store information that is used to classify later incoming packets (col 6 lines 62-64) and thus eliminate the requirement for continued analysis of packets from a permitted connection and accelerate the process of packet filtering, while still marinating the security of the private network (col 2 lines 5-19).

c. **In regards to claim 3,** Paunikar et al. in the method of claim 1 as modified above discloses,

- wherein said network session is a communication channel established between a source host (fig 1-#12) and a

destination host(figure 1-#18) over a network (figure 1-#10). (See Paunikar et al. [0030)

d. **In regards to claim 4**, Paunikar et al. in the method of claim 1 as modified above discloses,

- wherein the initial session determination includes comparing the event parameters of a newly received network event with the event parameters of any previously received network event, and if there is a match, the newly received event belongs to a same network session as those previously received matching events [0045].

e. **In regards to claim 5**, Paunikar et al. discloses in the method of claim 1 as modified above,

- wherein each of said one or more devices is associated with at least one network address translation rule (fig 2-#150, fig 2-#160), each rule comprising a pre-mapping parameter domain (i.e pool) and a post-mapping parameter domain for one or more event parameters [0027] [0034] [0036] [0039].

f. **In regards to claim 8,** Paunikar et al. discloses in the method of claim 1, wherein said categorizing includes:

- associating the network event with any previously received event (i.e. entry) in accordance with the initial session determination result [0045]; and

- associating the network event with any previously received event in accordance with the network address translation information obtained in said identifying [0045].

g. **In regards to claim 9**, Fink et al. in the method of claim 1 as modified above further discloses,

- wherein the predefined time is associated with a network event. Fink et al teaches a predefined time associated with a event (i.e. packet) Fink et al. (col 4 lines 51-64 col 10, lines 18-27).

h. **In regards to claim 10,** Paunikar et al. discloses in the method of claim 1,

- wherein the categorized network event and the identified other categorized network event belong to different categories (ie. protocols) during said categorizing [0040][0046].

i. **In regards to claim 11,** Paunikar et al. discloses the method of claim 1, wherein

- said processing is performed in accordance with the identified network address translation information for the network transmission path associated with the network event ([0026],[0046]lines 5-13, figure 4).

j. **In regards to claim 12,** Paunikar et al. discloses the method of claim 1, wherein

- said processing is performed in accordance with network address translation information received after arrival of the categorized network event [0026][0040][0045].

k. **In regards to claim 13,** Paunikar et al. discloses a network event grouping system, comprising:

vi. one or more central processing units for executing programs [0028];

vii. an interface ([0029] lines 7-10) for receiving network events; and

viii. a network event correlation engine module (fig 2) executable by the one or more central processing units [0028][0031], the module comprising:

- a plurality of data structures ([0028] lines 1-4) for storing a stream of network events, each network event including a set of event parameters in association with a network session that corresponds to a message being transmitted through a network ([0042] Lines 5-18);
- instructions for establishing a correlation when a network event in the stream belong to a same network session as another network event in the stream ([0045] lines 1-8);
- instructions for identifying information of network address translations performed by one or more devices along a network transmission path associated with a network event ([0045] lines 12-17);

- instructions for categorizing a network event in the stream in accordance with the event's network session relationship and/or the event's network address translation information[0040] [0045]); and
- instructions for invoking a categorized network event at a predefined time, wherein invoking comprises:

  (a) processing the categorized network event to identify another categorized network event, if any, belonging to a same network session as the categorized network event [0026] [0045],

  (b) grouping the categorized (i.e. based on protocol and network address) network event and the identified other categorized network event, if any, into a set [0046], and

  (c) assigning a unique identifier (i.e. IP address and protocol provided) to the set of events that includes the categorized network event ([0046]).

Paunikar et al., teaches a log that contains data on all current sessions, which includes session data such as times [0032]. However Paunikar et al. fails to explicitly teach predefined time to perform (a)-(c) above.

In related art, Fink et al. teaches a system that filters steam of events (i.e packets) and determines the destination to which the event will be forwarded to (col 2 lines 27-39). The system includes a source from which the stream of events initiates, a destination for receiving events and a NAT component (figure 1-#18, col 6 lines 65-67, col 7

lines 1-11) for filtering the events based on rules (col 2 lines 61-63). A NAT component (fig 1-#30) performs event (i.e packet) comparison to determine if the events belong to the same session (col 4 lines 26-33). The NAT component continues to monitor event activity as well as continues to perform the comparisons and if an event is not received within predefined period of time a timeout occurs and the connection is closed (col 4 lines 51-64).

It would have been obvious to one of ordinary skill in the art at the time of invention to perform (1)- (3) above of the Paunikar et al. system within a predefined time in order to, based on event activity, to prevent unexpected disconnection by determining whether to keep or close a session (col 10, lines 18-27) thereby only allowing permitted events on a private (i.e. protected) network (col 5 lines 41-59).

l. **In regards to claim 14**, Paunikar et al. discloses the system of claim 13 as modified above, wherein the set of event parameters include:

- source address, source port, destination address, destination, port, and network protocol [0033].

Fink et al. teaches a connection (i.e. session) as a plurality of parameters, which describe the data transmission to which a packet (i.e events) belongs. Parameters include source address and port of packet; destination address and port of the packet; protocol of the packet and interface from which the packet was received. The connection is used to classify the packet, and to determine whether the packet is permitted to enter and leave the protected network (col 6 lines 54-63).

It would be obvious to one of ordinary skill in the art at time of the invention to indicate the event parameters of Paunikar et al. as including such parameters in order to perform an initial session determination and store information that is used to classify later incoming packets (col 6 lines 62-64) and thus eliminate the requirement for continued analysis of packets from a permitted connection and accelerate the process of packet filtering, while still marinating the security of the private network (col 2 lines 5-19).

m. **In regards to claim 15,** Paunikar et al. in the system of claim 13 as modified above discloses,

- wherein said network session is a communication channel established between a source host (fig 1-#12) and a destination host(figure 1-#18) over a network (figure 1-#10). (See Paunikar et al. [0030)

n. **In regards to claim 16**, Paunikar et al. discloses in the system of claim 13 as modified above,

- wherein the instructions for establishing a correlation include comparing the event parameters of a newly received network event with the event parameters of any previously received network event, and if there is a match, the newly received event belongs to a same network session as those previously received matching events [0045].

o. **In regards to claim 17,** Paunikar et al. discloses in the system of claim 13 as modified above,

- wherein each of said one or more devices is associated with at least one network address translation rule (fig 2-#150, fig 2-#160), each rule comprising a pre-mapping parameter domain and a post-mapping parameter domain for one or more event parameters (Paunikar et al [0027] [0034] [0036] [0039]).

p. **In regards to claim 20,** Paunikar et al. discloses in the system of claim 13 as modified above, wherein said categorizing instructions include:

- associating the network event with any previously received event in accordance with the initial session determination result [0045]; and
- associating the network event with any previously received event in accordance with the network address translation information obtained in said identifying. [0045]

q. **In regards to claim 21**, Fink et al. in the system of claim 13 as modified above further discloses, wherein

- the predefined time is associated with a network event.

Fink et al teaches a predefined time associated with a packets (i.e. network events) Fink et al. (col 4 lines 51-64 col 10, lines 18-27).

r. **In regards to claim 22**, Paunikar et al. the system of claim 13, wherein

- the categorized network event and the identified other categorized network event belong to different categories (ie. protocols) during said categorizing[0040][0046].

s. **In regards to claim 23,** Paunikar et al. discloses the system of claim 13, wherein

- said processing is performed in accordance with the identified network address translation information for the network transmission path associated with the network event ([0026],[0046]lines 5-13, figure 4).

t. **In regards to claim 24**, Paunikar et al. discloses the system of claim 13 as modified above, wherein

- said processing is performed in accordance with network address translation information received after arrival of the categorized network event [0026][0040][0045].

u. **In regards to claim 25,** Paunikar et al. **discloses a** computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein ([0028] [0029] lines15-19), the computer program mechanism comprising:

ix. instructions for receiving and storing ([0031] a stream of network events, each network event including a set of event parameters in association with a network session that corresponds to a message being transmitted through a network ([0042] Lines 5-18);

x. instructions for establishing a correlation when a network event in the stream belong to a same network session as another network event in the stream ([0045] lines 1-8])

xi. instructions for identifying information of network address translations performed by one or more devices along a network transmission path associated with a network even([0045] lines 12-17);

xii. instructions for categorizing a network event in the stream in accordance with the event's network session relationship and/or the event's network address translation information([0040] [0045]); and

xiii. instructions for invoking a categorized network event at a predefined time [0032], wherein invoking comprises :

(1) processing the categorized network event to identify another categorized network event, if any, belonging to a same network session as the categorized network event([0026][0045]),

(2) grouping the categorized network event and the identified other categorized network event, if any, into a set, [0046] and

(3) assigning a unique identifier to the set of events that includes the categorized network event [0046].

Paunikar et al., teaches a log that contains data on all current sessions, which includes session data such as times [0032]. However Paunikar et al. fails to explicitly teach predefined time to perform (1)-(3) above.

In related art, Fink et al. teaches a system that filters steam of events (i.e packets) and determines the destination to which the event will be forwarded to (col 2 lines 27-39). The system includes a source from which the stream of events initiates, a destination for receiving events and a NAT component (figure 1-#18, col 6 lines 65-67, col 7 lines 1-11) for filtering the events based on rules (col 2 lines 61-63). A NAT component (fig 1-#30) performs event (i.e packet) comparison to determine if the events belong to the same session (col 4 lines 26-33). The NAT component continues to monitor event activity as well as continues to perform the comparisons and if an event is not received within predefined period of time a timeout occurs and the connection is closed (col 4 lines 51-64).

It would have been obvious to one of ordinary skill in the art at the time of invention to perform (1)- (3) above of the Paunikar et al. system within a predefined time in order to, based on event activity, to prevent unexpected disconnection by determining whether to keep or close a session (col 10, lines 18-27) thereby only allowing permitted events on a private (i.e. protected) network (col 5 lines 41-59).

b. **In regards to claim 26,** Paunikar et al. disclose the computer program product of claim 25 as modified above, wherein the set of event parameters include:

- source address, destination address, and network protocol [0033].

Paunikar et al. is silent on source port and destination port.

Fink et al. teaches a connection (i.e. session) as a plurality of parameters, which describe the data transmission to which a packet (i.e events) belongs. Parameters include source address and port of packet; destination address and port of the packet; protocol of the packet and interface from which the packet was received. The connection is used to classify the packet, and to determine whether the packet is permitted to enter and leave the protected network (col 6 lines 54-63).

It would be obvious to one of ordinary skill in the art at time of the invention to indicate the event parameters of Paunikar et al. as including such parameters in order to perform an initial session determination and store information that is used to classify later incoming packets (col 6 lines 62-64) and thus eliminate the requirement for continued analysis of packets from a permitted connection and accelerate the process of packet filtering, while still marinating the security of the private network (col 2 lines 5-19).

c. **In regards to claim 27**, Paunikar et al. in the computer program product of claim 25 as modified above,

- wherein said network session is a communication channel established between a source host (fig 1-#12) and a destination host(figure 1-#18) over a network (figure 1-#10). (See Paunikar et al. [0030)

d. **In regards to claim 28,** Paunikar et al. discloses in the computer program product of claim 25 as modified above,

- wherein the instructions for establishing a correlation include comparing the event parameters of a newly received network event with the event parameters of any previously received

network event, and if there is a match, the newly received event belongs to a same network session as those previously received matching events [0045].

e. **In regards to claim 29,** Paunikar et al. discloses in the computer program product of claim 25 as modified above,

- wherein each of said one or more devices is associated with at least one network address translation rule (fig 2-#150, fig 2-#160), each rule comprising a pre-mapping parameter domain and a post-mapping parameter domain for one or more event parameters [0027] [0034] [0036] [0039].

f. **In regards to claim 32, Paukinar** et al. discloses in the computer program product of claim 25, wherein said categorizing instructions include:

- associating the network event with any previously received event in accordance with the initial session determination result [0045]; and
- associating the network event with any previously received event in accordance with the network address translation information obtained in said identifying [0045]

g. **In regards to claim 33,** Fink et al. in the computer program product of claim 25 as modified above further discloses,

- wherein the predefined time is associated with a network event.

Fink et al teaches a predefined time associated with a event (i.e. packet) Fink et al. (col 4 lines 51-64 col 10, lines 18-27).

v. **In regards to claim 34,** Paunikar et al. discloses the computer program product of claim 25,

- wherein the categorized network event and the identified other categorized network event belong to different categories (i.e. protocols) during said categorizing [0040][0046].

w. **In regards to claim 35,** Paunikar et al. discloses the computer program product of claim 25 as modified above, wherein

- said processing is performed in accordance with the identified network address translation information for the network transmission path associated with the network event ([0026],[0046]lines 5-13, figure 4).

x. **In regards to claim 36,** Paunikar et al. the computer program product of claim 25 as modified above, wherein said processing is performed in accordance with network address translation information received after arrival of the categorized network event [0026][0040][0045].

Allowable Subject Matter

1. Claim 18, 30 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

2. Claim 6,7, 19, 31 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Data Processing System Handling Fault Recovery of a Network

- Angelino, Robert et al. (US 20040193943 A1) Multiparameter network fault detection system using probabilistic and aggregation analysis

Computer Network Monitoring

- Lewis, Lundy M (US 2004/0153533 A1) Method and apparatus for a comprehensive network management system
- Feridun; Metin et al. (US 6336139 B1) System, method and computer program product for event correlation in a distributed computing environment
- Syvanne, Tuomo et al. (US 20030149766 A1) Firewall configuration validation

Security of a Computer Network

- Yang, Xuechen (US 20030088788 A1) System and method for managing dynamic network sessions
- Scheidell, Michael (US 20040098623 A1) Intrusion detection system
- Zuk, Nir et al. (US 20030154399 A1) Multi-method gateway-based network security systems and methods
- Douglas, Kevin (US 20040049693 A1) Modular system for detecting, filtering and providing notice about attack events associated with network security
- Bowman-Amuah; Michel K. (US 6324647 B1) System, method and article of manufacture for security management in a development architecture framework

Path Finding or Routing: Combined circuit switching and packet switching

- Bhatia; Rajiv et al. (US 6829239 B1) Apparatus and methods for determining the correct workstation within a LAN for a LAN modem to route a packet

Computer-to-Computer Addressing

- Cunningham; Timothy et al. (US 6493765 B1) Domain name resolution in a network having multiple overlapping address domains
- Takeda, Yutaka et al. (US 20040139228 A1) Peer-to-peer (P2P) connection despite network address translators (NATs) at both ends

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carolyn F. Fleary whose telephone number is (571) 572-721. The examiner can normally be reached on 8:30 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (571)272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Dung C. Dinh
Primary Examiner

Carolyn F Fleary
Examiner
Art Unit 2152

***

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.